Policy Central (Tech Preview)

Version: 2024.3.0.0

Copyright AppViewX, Inc.

Trademarks

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.2	Updated draft of document for release 2024.3.0.0	September 2025
1.1	Updated draft of document for release 2024.2.0.0	June 2025
1.0	Initial draft of policy central document for release 2024.1.0.0	March 2025

About the Documentation

This section includes the following guides that will give you an overview of Policy Central.

Audience

This guide is intended for everyone deploying AppViewX One product's for managing their certificates.

Third-Party Software Acknowledgments

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Policy Central

AppViewX's Policy Central is a comprehensive, centralized policy management platform designed to streamline compliance, enhance security, and enforce standardization across organizations. It provides a flexible framework for customizing policies to align with both organizational standards and specific operational needs. Its adaptability ensures seamless integration into existing workflows, driving improvements in security and compliance processes.

In version 2024.0.0 FP1, Policy Central enables policy creation for Certificate Enrollment compliance. Future releases will expand support to include additional Certificate Lifecycle Management (CLM) actions like renewal and regenerate.

Important: Policy Central is a unified policy management system introduced as a Tech Preview feature in AppViewX. Enabling access to Policy Central will also grant the required permissions for the CERT+, Platform, and Automation modules.

Key Features:

- Enforce compliance in the certificate enrollment process through tailored forms and customizable approval levels.
- Provide an enhanced user experience with a custom self-service page designed for ease of use and accessibility.

Chapter 2: Prerequisites

At present, Policy Central supports only the Certificate Enrollment Policy, so a CERT+ license is required to create a policy.

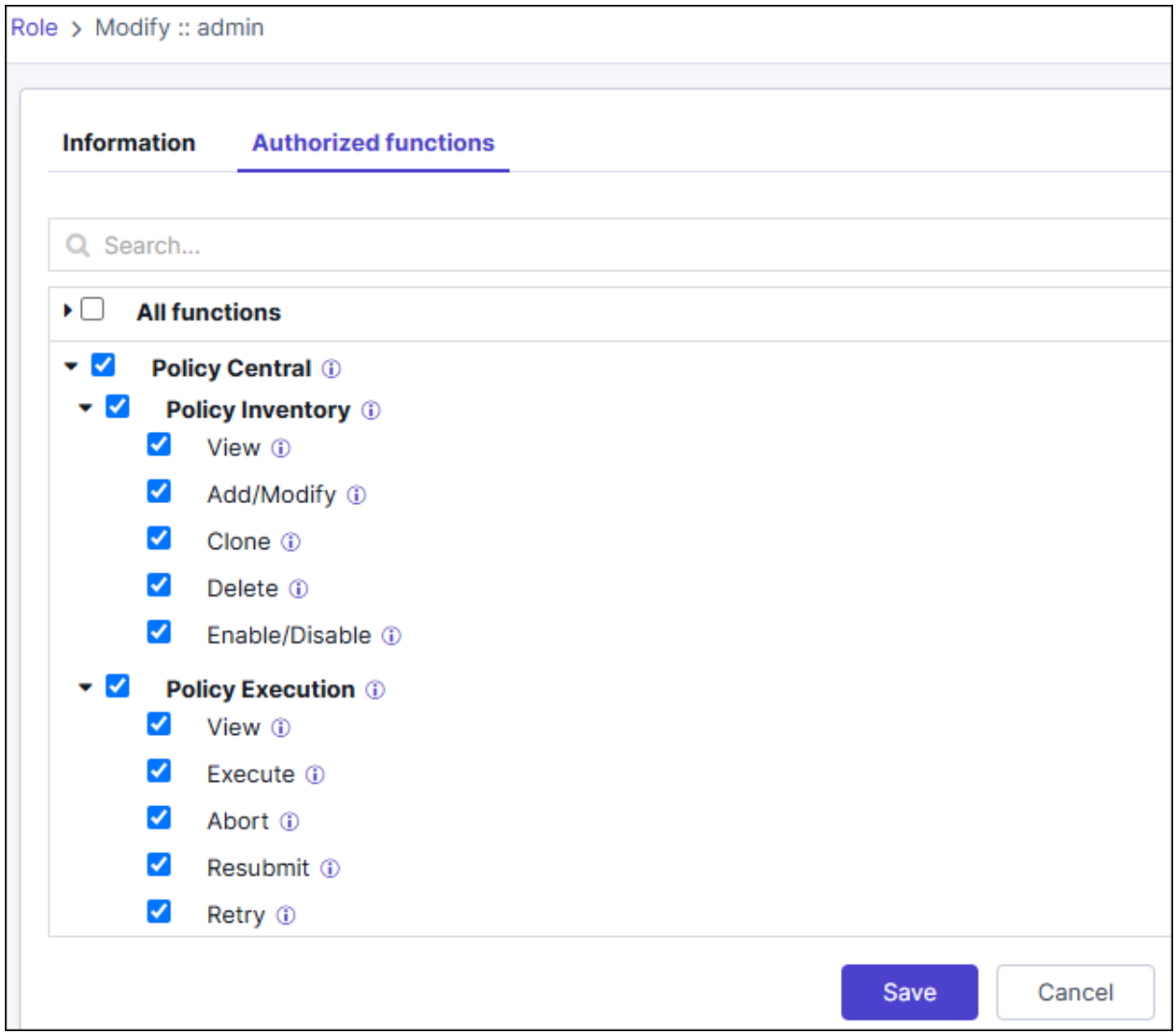
- Access to Policies

Enabling Policy Central

By default, Policy Central is disabled for the admin role. Users can enable this permission as needed.

To enable Policy Central, follow these steps:

1. Go to **(Menu)** > **Platform** > **IDENTITY** > **Role**.
   You will be redirected to the **Role** page.
2. Click the role name to enable the ACF permission.
   You will be redirected to the **Modify :: [RoleName]** page, with the **Information** tab open by default.
3. Switch to the **Authorized Functions** tab.
4. To enable **Policy Central**, select the checkbox for **Policy Central**.



Note: Enabling access to Policy Central will also grant the necessary permissions for the Certificate, Platform, and Automation modules.

Note: Users with Policy Central ACF permissions can create or edit KUBE or CERT policies in Policy Central without having the specific ACF permissions required for KUBE and CERT.

5. **Policy Inventory** Permission define the access control and user privileges required to manage and interact with policies. Users can be granted access to the Policy Inventory based on the permissions assigned to their role.

Permission	Description
View	Grants access to view the inventory.
Add/Modify	Allows users to create and modify policies.
Clone	Allows users to clone existing policies
Delete	Allows users to delete policies.
Enable/Disable	Allows users to change the status of a policy (enable or disable).

6. **Policy Execution** Permission define the access control and user privileges required to manage and interact with policies. A user can be granted execution permissions based on the access assigned to their role.

Permission	Description
View	Grants access to view the Policy Requests History.
Execute	Allows users to execute policies.
Abort	Allows users to abort an ongoing policy request.
Resubmit	Allows users to resubmit a failed execution.
Retry	Allows users to retry an execution.

7. Click **Save**.

Onboard a Certificate Authority

To create a policy, the required Certificate Authority must be onboarded. Currently, Policy Central supports the Certificate Enrollment Policy for the following Certificate Authorities:

- Digicert
- MSCA
- GlobalSign / GlobalSign MSSL
- Let's Encrypt
- Sectigo
- InCommon.

CA Policy Modifications

The existing CA policy in CERT+ is integrated with the certificate enrollment process. To ensure seamless experience with Policy Central, specific configuration changes must be made to the CA policy.

1. Go to **(Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. For all CA policies in CERT+ change.
   - **Policy Enforcement Type** from **Strict** to **Suggestive**.
   - **Certificate Requests Need Approval?** from **on** to **off**.
   - **Enable Access to Private Key?** from **off** to **on**. (If the certificate, along with its private key, needs to be mailed through Policy Central).

Configure SMTP

Policy Central currently supports approvals and notifications via email only. To send and receive approval/notification emails, SMTP settings must be configured.

1. Go to **(Menu)** > **Platform** > **SYSTEM ADMINISTRATION** > **SMTP**.
   The **Settings :: SMTP** page is displayed.
2. **Configure the SMTP Settings**.

Enable the Default Email Template

By default, Policy Central uses the **AppViewXDefault** email template for sending approval and notification emails. This template must be enabled under the **Platform** module.

1. Go to **(Menu)** > **Platform** > **SYSTEM ADMINISTRATION** > **Themes and Personalization**.
   The **Settings :: Theme** page is displayed with the **Logo** tab open by default.
2. Click the **Email Attachment Customization** tab.
3. Under the **Email Template** section, select **AppViewXDefault**.
4. Click the **Edit** icon.
5. Turn on the toggle to use **AppViewXDefault** template.
6. Click **Update**.
   The **AppViewXDefault** template will be set as the **Default** email template.

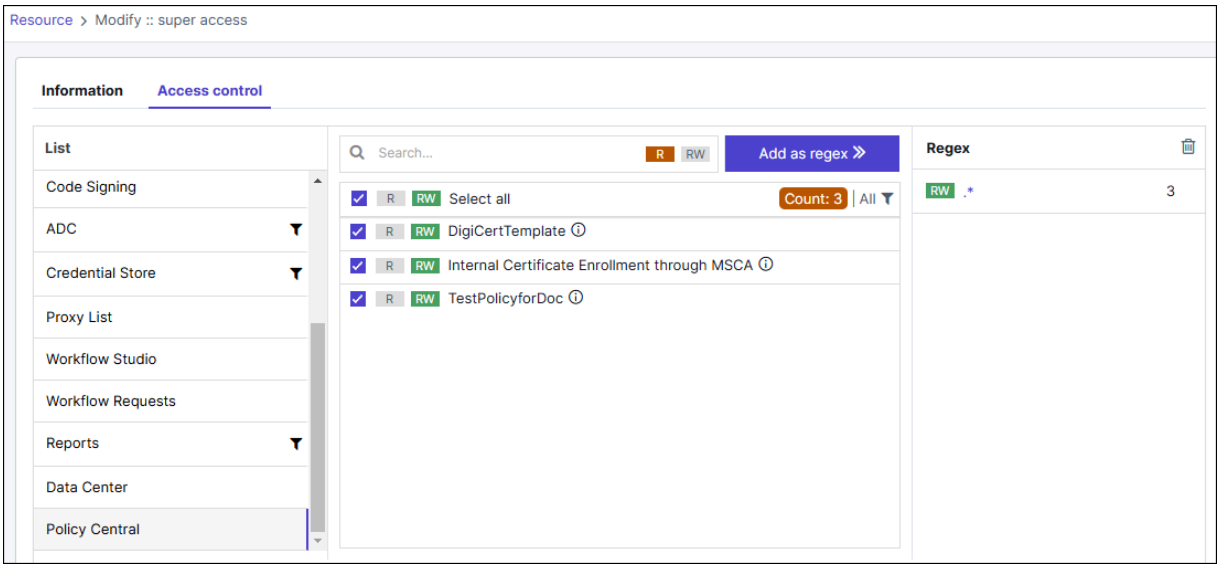
Access to Policies

Policy access can be managed in the Policy Inventory using the User Access option. If access needs to be granted to multiple policies based on name patterns or if specific access is required for multiple policies, this can be handled in the **Platform** module.

1. Go to **(Menu)** > **Platform** > **IDENTITY** > **Resource**.
   The **Resource** page is displayed.
2. Click the resource name to which you want to grant policy access.
   The **Information** tab is displayed.
3. Click the **Access control** tab to add/remove the items from the resource.
4. Click the respective resource in the left pane.
   The list of items is displayed on the right with the checkboxes and the **R** or **RW** options enabled/ disabled for the items.

> **Note:** You can modify Read (R) and Read/Write (RW) permissions associated with a resource.

5. Select/Clear the checkbox(es) for the item(s) you want to associate with/dissociate from the resource.



- A regex pattern can be created to assign R/RW access. All policies matching the regex will be granted the specified access.
- Multiple policies can also be selected and given R/RW access.

a. Click **R (Read-only)** to assign read-only permissions.

b. Click **RW (Read and Write)** to assign read and write permissions.

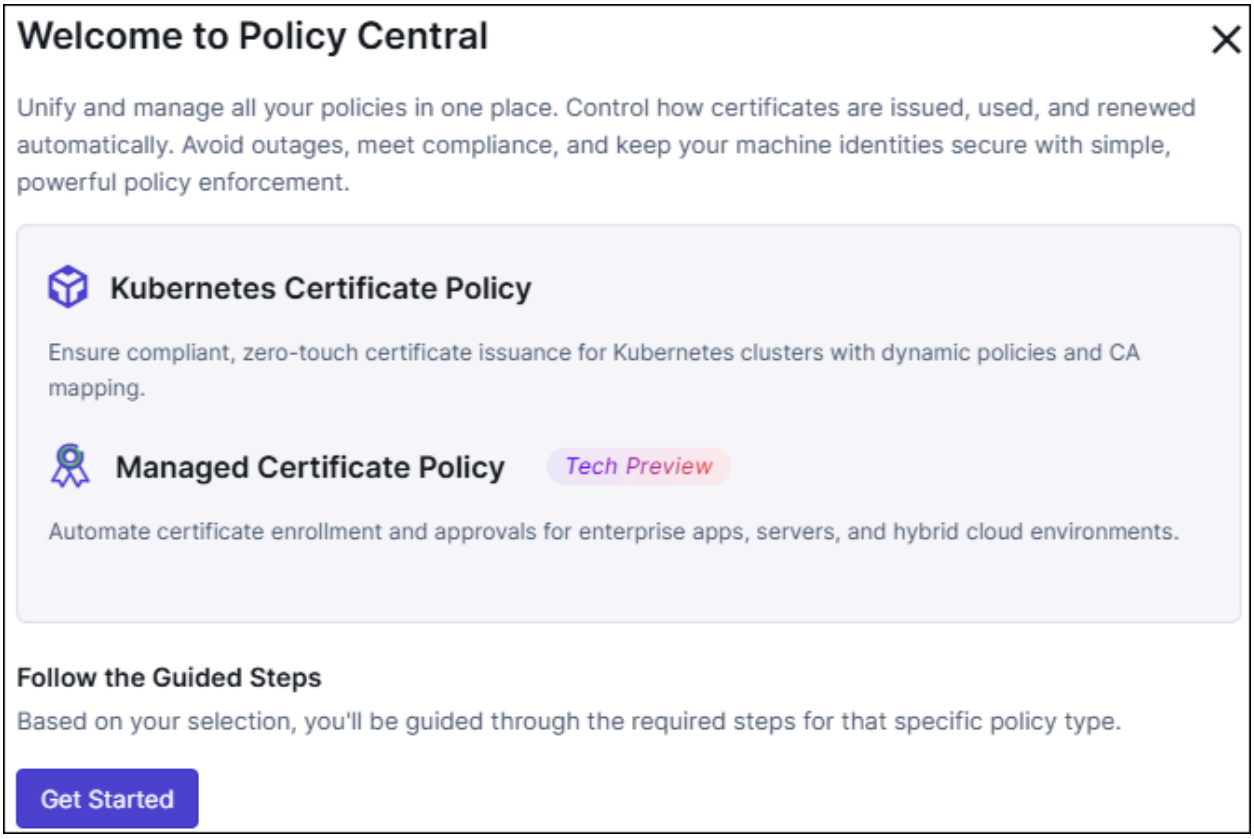
6. Click **Save**.

Chapter 3: Getting Started

To enable Policy Central, please refer Enabling Policy Central.

A policy in Policy Central outlines the approved rules and steps for certain actions to ensure they meet established standards and regulations. For example, new certificates may be required to use a particular key type, or there may be specific naming conventions for common names. Additionally, the certificate enrollment process could require two distinct approval levels.

Once Policy Central is enabled, clicking the **Policy Central** option under **(Menu)** dropdown will take you to the Policy Inventory page, where the **Welcome to Policy Central** popup will be displayed.

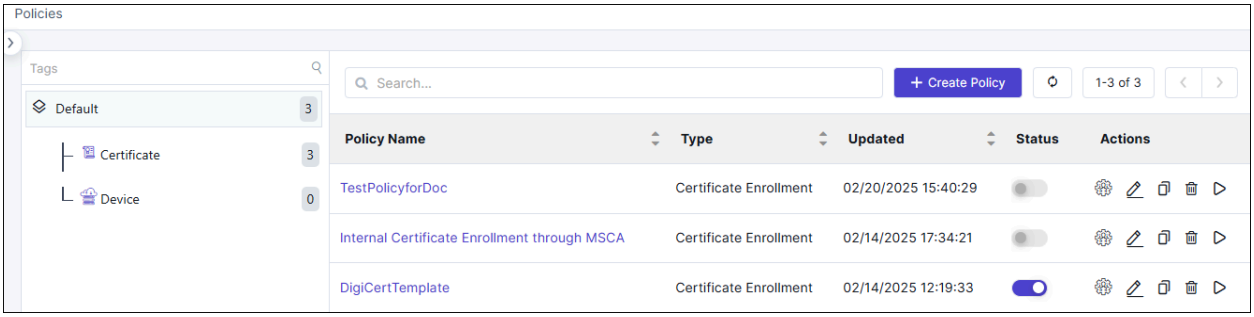


Click **Get Started** to create your first policy.

The Create Policy pop-up is displayed. To configure the policy refer the following steps here.

Chapter 4: Policy Inventory

The Policy Inventory serves as a centralized repository that lists all created policies. It provides key details such as policy names, types (e.g., certificate enrollment), status (enabled/disabled), and available actions, including granting user access, editing, deleting, cloning, and executing policies. This section enables administrators to efficiently track and manage policies, ensuring compliance with organizational standards.

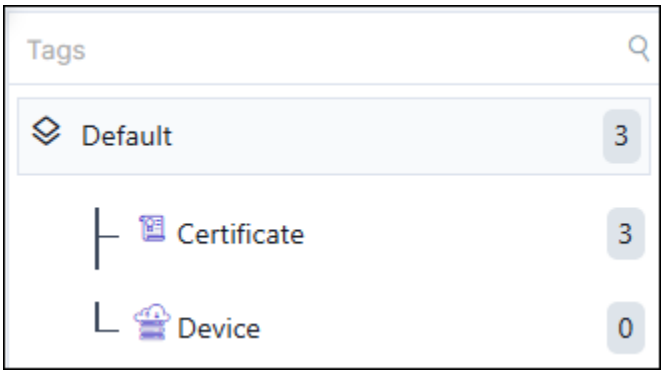


Here are some key elements displayed in the Policy Inventory:

- Tags
- Create Policy
- Policy Actions
- Creating a Cluster Policy Using Policy Central

Tags

Tags are used to logically group the policies, simplifying their organization and management based on specific criteria. Users can map a policy to a particular tag for better classification and easier retrieval. Tagging enhances the ability to filter and search policies efficiently, particularly in environments with large number of policies. With well-organized tags, organizations can optimize policy management and enforcement.

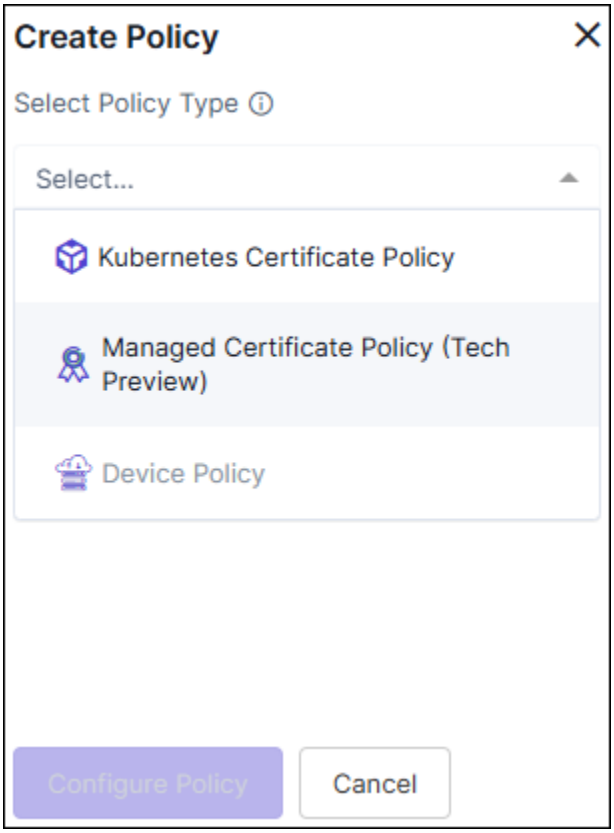


Create Policy

Policies can be created for various Certificate Lifecycle Management actions to ensure compliance and align with organizational standards.

To create a new policy:

1. Go to **(Menu)** > **Policy Central** > **POLICY MANAGEMENT** > **Policies**.
   The **Policy Inventory** page is displayed.
2. On the **Policy Inventory** page, click **+ Create Policy** **(+ Create Policy)**.
   The **Create Policy** popup is displayed.
3. Select **Policy Type** from the dropdown.



Choose the appropriate type of policy based on your specific requirements:

a. **Kubernetes Certificate Policy**

Creating a Cluster Policy.

b. **Managed Certificate Policy (Tech Preview)**
c. **Device Policy**

4. Enter the following details to configure the policy.

Field description for Create Policy

Fields	Description
***Policy Name**	Enter a policy name that can include alphabets, numbers, and the special characters - and _
Description	Enter the description for the policy.
***Select a Tag**	Select an existing tag from the dropdown or create a new one. **Note:** Selecting the appropriate policy type allows you to group policies logically, simplifying organization and management based on specific criteria.
**: Mandatory fields*	

5. Click **Configure Policy**.
   Once the policy is created successfully, a confirmation message will appear, and you will be redirected to the **Configure Policy** page.

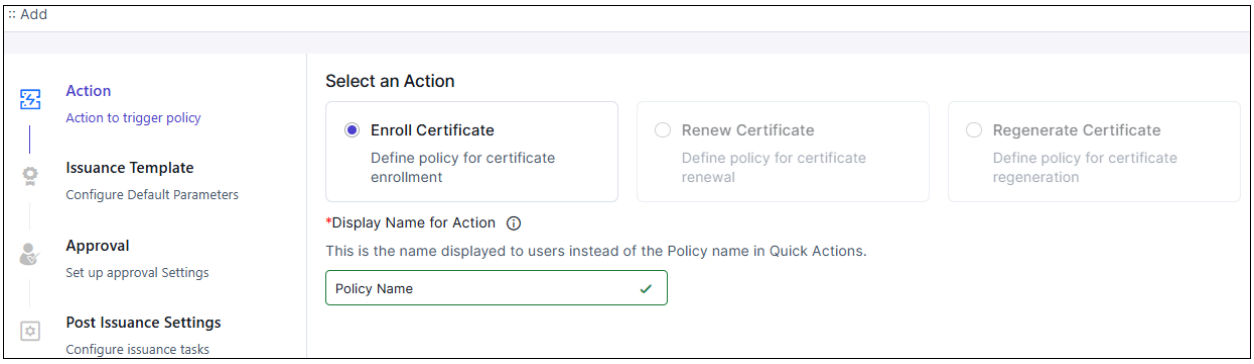
Configuring Policy

The policy creation process is made up of different functional blocks, with each block in the policy flow known as a component. The components that form a Certificate Enrollment Policy are as follows:

Action > **Issuance Template** > **Approval** > **Post Issuance Settings**

Action to Trigger Policy

The Action Component enables to choose an action, such as **Enroll Certificate**, **Renew Certificate**, or **Regenerate Certificate**. A Display Name for the action must be provided, which will appear in Quick Actions to assist users in easily executing the policy.



To configure trigger policy:

1. Select an **Action**.
   - **Enroll Certificate**

     Currently, Policy Central supports the creation of certificate policies only for the Enroll Certificate action.

   - Renew Certificate
   - Regenerate Certificate.
2. Enter the name to be displayed to users in **Quick Actions** under **Policy Request**, instead of the policy name.
3. Click **Next**.

   The **Issuance Template** screen is displayed.

Issuance Template

An issuance template is a customizable form that defines how certificate request fields are created and processed. It enables administrators to control the information collected during the certificate request process and how it is validated.

To configure the issuance template:

1. Choose from the list of supported CA vendors (e.g., DigiCert, Entrust, etc.)
2. To customize the issuance template as per the requirement.
   a. Select the template to be customized from the list.
   b. Validate the available parameters and click **Confirm** to import the template.

Note:

- These templates include commonly used field configurations.
- Templates are designed to match vendor-specific certificate requirements.
- When you click **Confirm** to apply a template, any previous customizations will be replaced by the new template's configurations.

c. Enter the required details for each parameter.

d. To customize the existing fields:

i. Click **(Settings)** icon.

The **Select/Text Box** popup is dispalyed

ii. **Field Customisation**

Fields	Description
Hide Field	Enable the toggle to completely remove field from view when not needed.
Read Only	Enable the toggle to display field values while preventing modifications. **Note:** This field is disabled when the Hide Field toggle is turned on.
Set as mandatory	Enable the toggle to ensure critical information is always provided. **Note:** This field is disabled when the Hide Field toggle is turned on.
*Label name	Customize field labels for clarity.
Help Tooltip	Provide additional guidance with hover tooltips.
*: Mandatory fields	

Note: For more details on custom regex validation, click here.

iii. Click **Save**.

The field customisation is saved.

iv. Click **(Hide/Unhide)** icon.

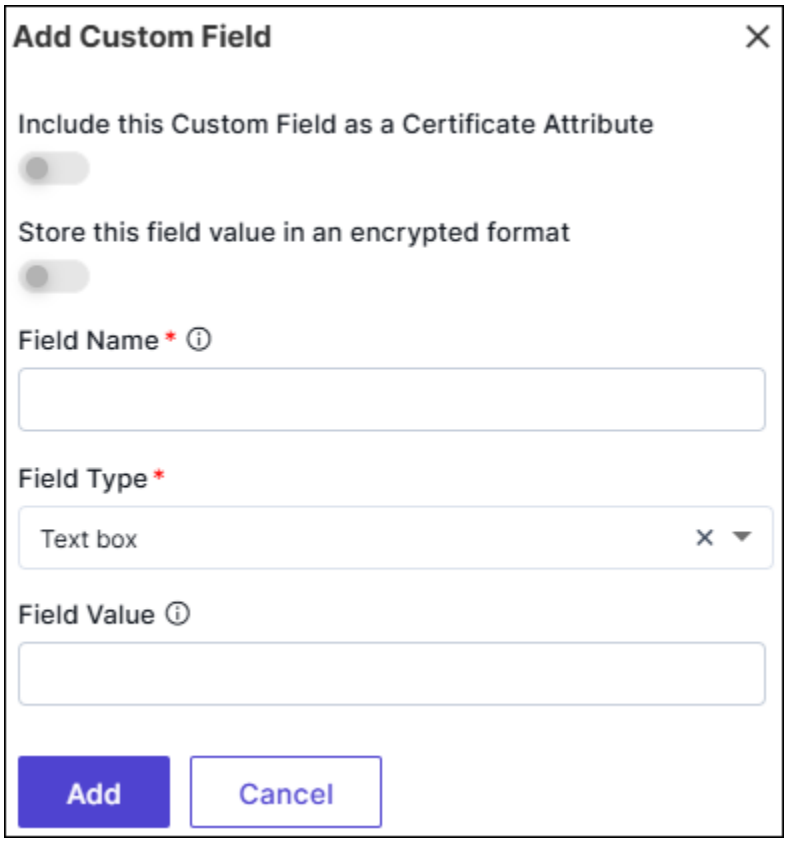
To hide/unhide the field directly without going to settings.

e. To add new custom fields:

You can add new custom fields to the Issuance Template for certificate attributes. When adding a custom field, the following options are available:

i. Click **+ Add Custom Field**.

The **Add Custom Field** popup is displayed.



Fields	Description
Include this Custom Field as a Certificate Attribute	Enable the toggle to **Include this Custom Field as a Certificate Attribute** in the certificate attributes page and inventory.

Fields	Description
	Note: • When enabled, only Text Box and Select Box field types are supported under **Field Type**. • When disabled, all field types are available under **Field Type**.
Store this field value in an encrypted format	Enable the toggle to **Store this field value in an encrypted format**. **Note:** • To encrypt sensitive field data for secure storage. • Encrypted fields are protected in the database.
Field Name	Enter a unique identifier for the field in alphanumeric format, required for system identification and processing.
***Field Type**	Select **Field Type** from the dropdown.Standard field types include: • Text Box • Text Area • Select Box • Multi-select Box • Check Box • Radio Button **Note:** When **Include this Custom Field as a Certificate Attribute**toggle is enabled, only **Text Box** and **Select Box** field types are supported.
Field Value	Default values can be provided for the field. For multiple values, use comma-separated values.
**: Mandatory fields*	

ii. Click **Add**.

The Custom field is added under **Certificate Attributes**.

3. To use the available saved templates without any changes.

   The pre-configured master templates offer commonly used field configurations, can be customized to meet specific needs, save time on setup, and serve as a foundation for various certificate types.

   a. Choose the required vendor from the list to view the available templates for that specific vendor.

   > **Note:**
   > • You can also search for templates by typing two or more characters in the search bar.
   > • If this is your first time configuring the policy, only the master template will be available.

   b. Click **[Required Template]**.

   The **Import Issuence Template** popup is diaplayed.

   c. Validate the template configurations and click **Confirm** to apply it.

   The **Issuence Template** details will be dispalyed.

   > **Note:** When you click **Confirm** to apply a template, any previous customizations will be replaced by the new template's configurations.

   d. Enter the required details for each parameter.

4. Click **Preview**, to preview the Issuance Template. (Optional)

   For more details on preview option in issuance template, click here.

5. Click **Variables**, to view the available dynamic variables. (Optional)

   For more details on dynamic variables, click here.

6. To Save the customized issuance template, click **Save as New**.

   > **Note:** The **Save Template** button appears only after making modifications to any template, while the **Update Existing** option is exclusively available for templates previously saved by users, not for out-of-box templates.

7. To modify existing saved template with new customizations, click **Update Existing**.
8. Click **Next**.

   The **Approval** page is displayed.

Form Building Capabilities

The **Issuance Template** component uses a form builder to dynamically add or modify fields, allowing a preview of how it will appear to a certificate requestor.

Field Types

The template component supports various field types to capture different kinds of information:

- Text Input
  - Single-line text entry for basic information.
  - Password-protected fields for sensitive data.
  - Support for regex validation rules.
- Selection Fields
  - Dropdown menus for single selection.
  - Multi-select boxes for multiple choices.
  - Radio buttons for exclusive options.
  - Checkboxes for multiple toggles.
- Text Area
  - Multi-line text entry for longer content.

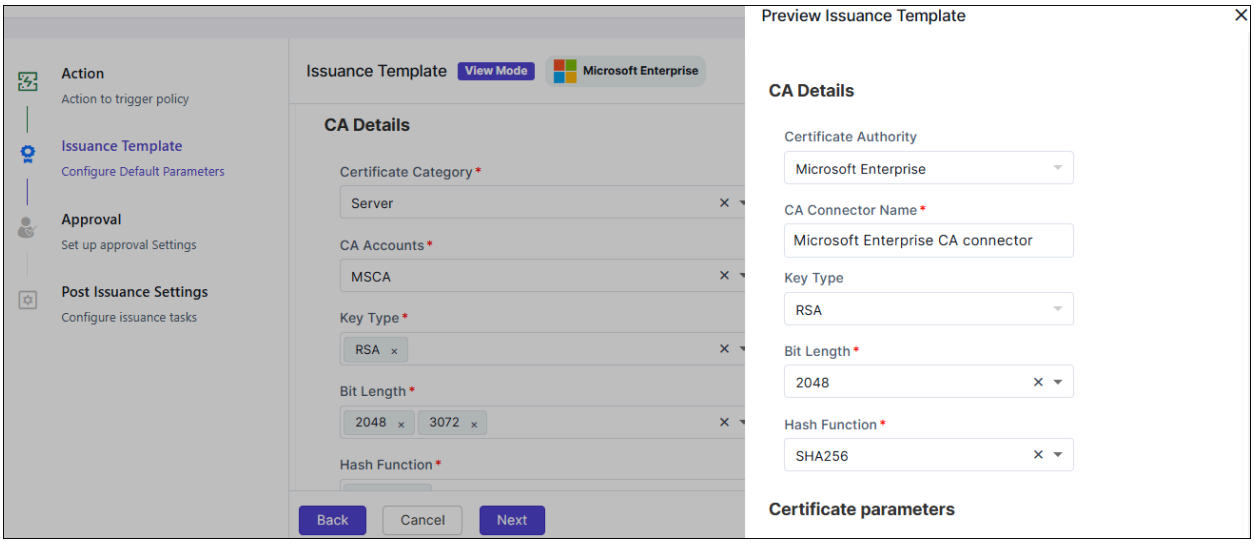
Preview Option in Issuance Template

On the policy creation page, the Preview Option is available in the Issuance Template page, allowing the policy creator to see how the page will look to the end-user when they use the policy to create a request.

Preview Behavior:

- **Hidden fields** > Not displayed.
- **Read-only fields** > Disabled for editing.
- **Mandatory fields** > Marked with an asterisk (*).
- **Dynamic Variables** > Replaced with real values based on the **current user's (policy creator's)** context.

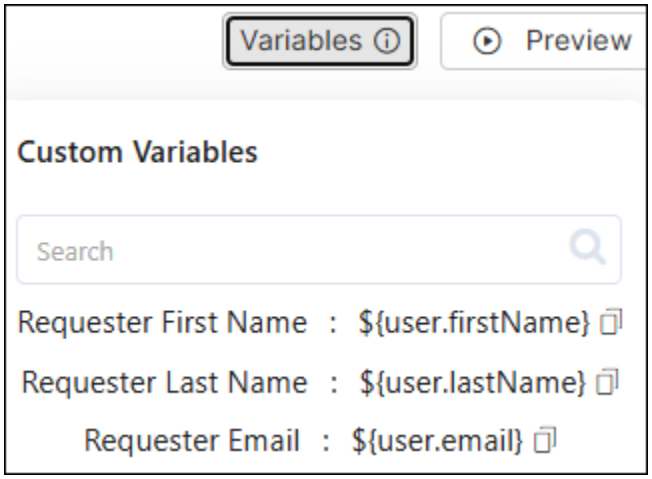
This feature helps policy creators check how the policy will apply configured rules (such as field visibility, editability, required fields, and dynamic variables) before finalizing it.



Dynamic Variables Support

Text Input and Text Area fields support dynamic variables:

- Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}).
- Variables can be inserted into text content.
- At runtime, variables are replaced with actual values.
- Supports copy-paste of variables from the provided list.



Field Customization Options

Validation Rules

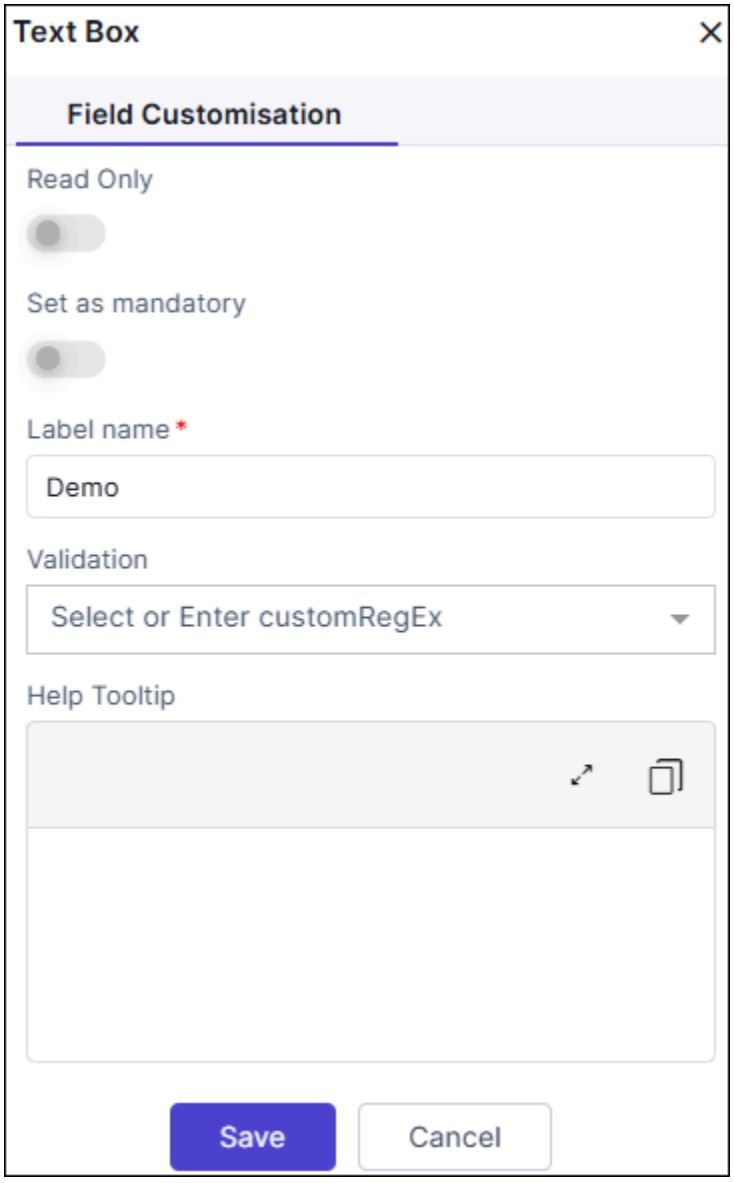
Policy Central provides pre-configured out-of-box validations and support for custom regex patterns to ensure data accuracy and format consistency.

Out-of-Box Validations:

1. **Email**
   - Regex: `^([a-z0-9_.-]+)@([da-z.-]+).([a-z.]{2,6})$`
   - Validates:
     - Username: Allows lowercase letters, numbers, underscore, dots, hyphens, and single @ separator.
     - Domain: Allows letters, dots, and hyphens.
     - Top-level domain: 2-6 characters long.
   - Valid examples: user1@example.com, user123@domain-name.co.
2. **FQDN with atleast two dots**
   - Regex: `^[(a-zA-Z0-9)]+[.]{1}[(a-zA-Z0-9)]+[.]{1}[(a-zA-Z0-9)]+([.]{1}[(a-zA-Z0-9)]+)*$`
   - Validates:
     - Requires a minimum three parts separated by dots.
     - Allows letters (both cases) and numbers in each part.
     - Can have additional subdomains.
   - Valid examples: sub.domain.com, example.org.uk.
3. **FQDN with two dots**
   - Regex: `^[(a-zA-Z0-9)]+[.]{1}[(a-zA-Z0-9)]+[.]{1}[(a-zA-Z0-9)]+$`
   - Validates:
     - Requires exactly three parts separated by two dots.
     - Allows letters (both cases) and numbers in each part.
   - Valid examples: www.testing.com.
4. **IP Address**
   - Regex: `^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]).){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])$`
   - Validates:
     - Four octets separated by dots.
     - Each octet must be between 0-255.
     - Properly handles all valid IP ranges.
   - Valid examples: 192.168.1.1, 10.0.0.0, 255.255.255.255
5. **IP Address with Port**
   - Regex: `^((([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]).){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]):(6553[0-5]|655[0-2]d|65[0-4]d{2}|6[0-4]d{3}|5d{4}|[0-9]d{0,3}))$`
   - Validates:
     - Valid IP address (as above).
     - Followed by colon and port number.
     - Port number must be between 0-65535.
   - Valid examples: 192.168.1.1:8080, 10.0.0.0:443

6. **Numbers**
   - Regex: `^[0-9]*$`
   - Validates:
     - Allows only numeric digits.
     - Can be empty or any length.
   - Valid examples: 123, 456789
7. **Port**
   - Regex: `^([1-9][0-9]{0,3}|[1-5][0-9]{4}|6[0-4][0-9]{3}|65[0-4][0-9]{2}|655[0-3]|6553[0-5])$`
   - Validates:
     - Numbers between 1-65535.
     - Properly validates all valid port ranges.
     - Prevents invalid port numbers.

- Valid examples: 80, 443, 8080, 65535

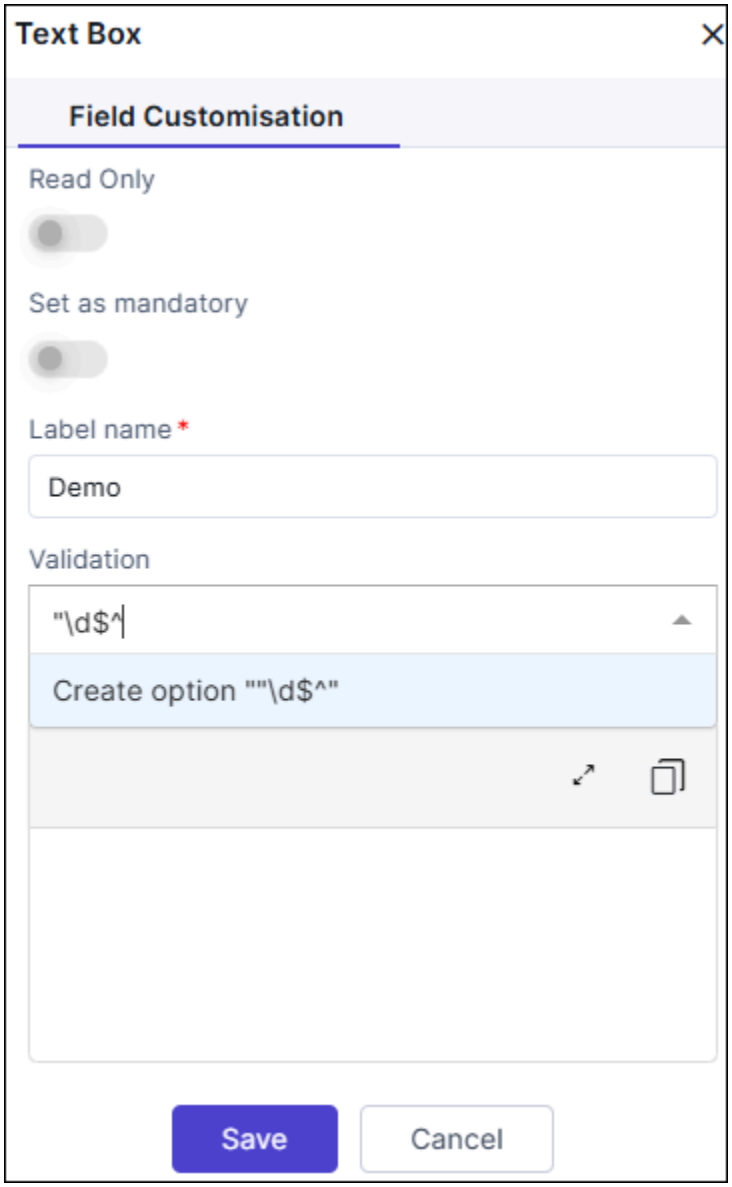


Custom Regex Validation

Administrators can create custom regex patterns for specific validation requirements by:

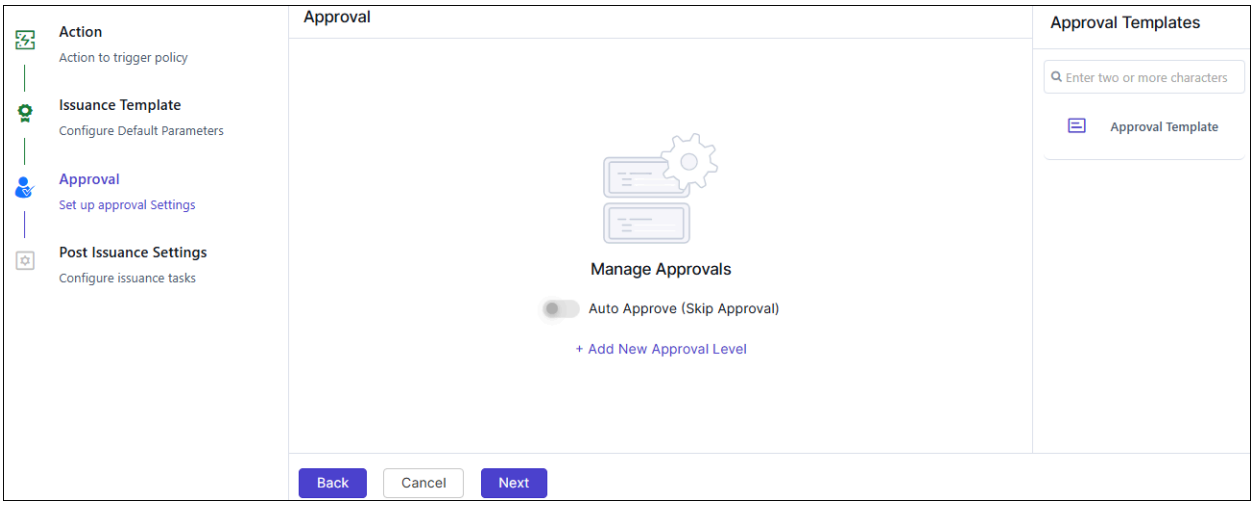
- Using the Creatable option.
- Entering a custom regex pattern.

• Testing the pattern against sample data before implementation.



Approval

The Approval Component allows multiple approval levels within Policy Central, so administrators can set up policies that require approvals. Each approval level can have different types of approvers, and the system makes sure requests are handled smoothly. You must set up at least one approval level, or enable auto-approval, which skips the approval process and executes the policy right away.

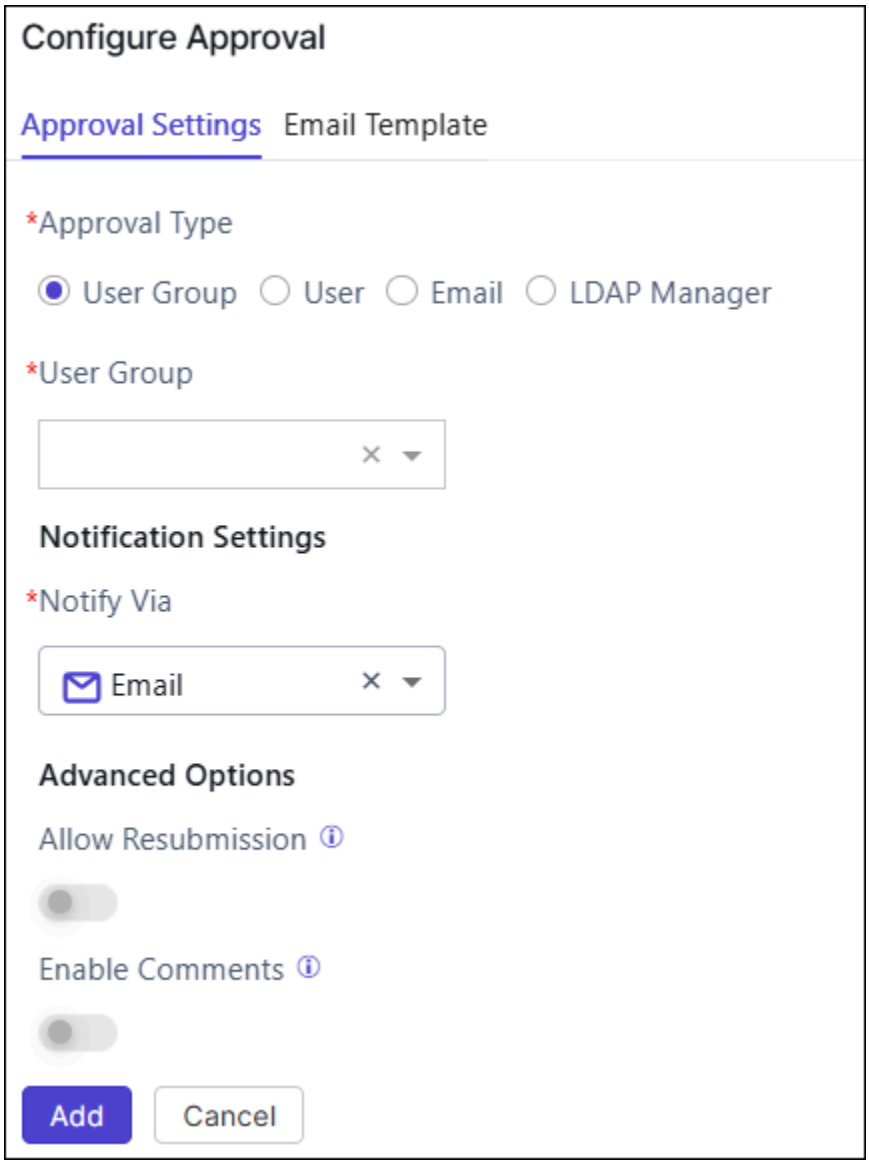


1. In the Manage Approvals, click one of the following:
   - Auto Approve (Skip Approval), to auto approve.
   - Add New Approval Level, to add new approval level.

   Note: This is displayed when Auto approve is disabled.

   a. Click Add New Approval Level, to add new approval level.

      The Configure Approval screen is displayed with Approval Settings tab.



b. In the Approval Settings, enter the following details:

Field	Description
*Approval Type	Choose one of the following: • **User Group** • **User** • **Email** • **LDAP Manager**

Field	Description
*User Group	**Note:** This field is displayed if approval type is selected as User Group. Any user within the selected user group can approve the request.
*User	**Note:** This field is displayed if approval type is selected as User. Multiple users can be assigned as approvers for the level.
*Email	**Note:** This field is displayed if approval type is selected as Email. Static email addresses are provided for approvals. Multiple email addresses can be added, separated by commas.
*LDAP Server	**Note:** This field is displayed if approval type is selected as LDAP Manager. A default query is used to fetch the LDAP manager from the LDAP server. The requester's LDAP manager is automatically assigned as the approver.
Customize LDAP Query	**Note:** This field is displayed if approval type is selected as LDAP Manager. Custom queries can be defined by configuring:
User Filter Attribute	**Note:** This field is displayed when Customize LDAP Query toggle is enabled. Identifies the requester's login name in LDAP.

Field	Description
User Return Attribute	**Note:** This field is displayed when Customize LDAP Query toggle is enabled. Maps to the manager reference in the user context.
Manager Filter Attribute	**Note:** This field is displayed when Customize LDAP Query toggle is enabled. Identifies the manager document.
Manager Return Attribute	**Note:** This field is displayed when Customize LDAP Query toggle is enabled. Identifies the manager's email in LDAP.
**: Mandatory fields*	

c. In the Notification Settings section, select Email from the notify via dropdown.

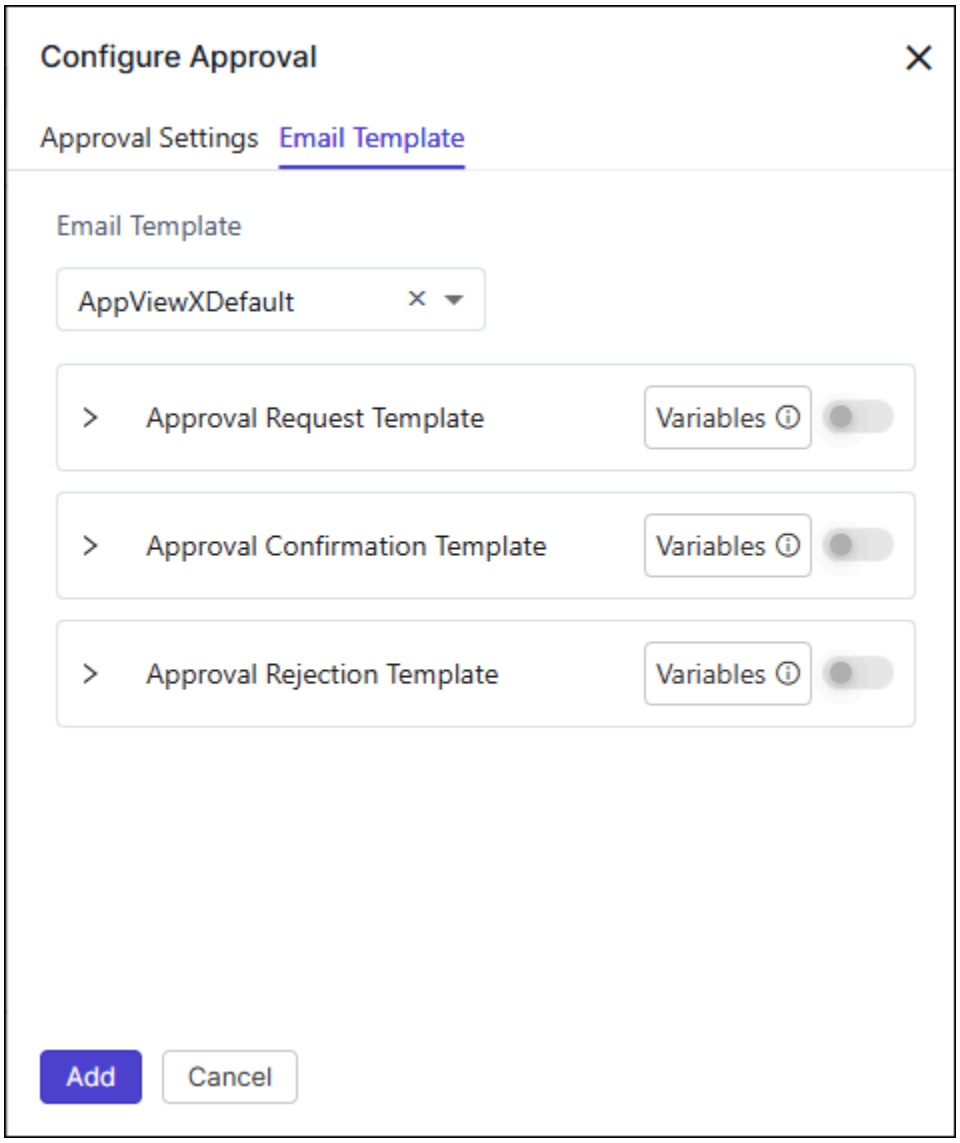
d. Advanced Options section, select the following toggle:

- **Allow Re-submission:** On enabling, allows the resubmission of the policy request.
- **Enable Comments:** On enabling, approver can add comments to the policy.

2. As part of the **Approval** step for creating a policy, you can select the required approval email template under the **Email Template** tab and customize it as required.

a. To select/customize email templates, Click **Email Template**.

The **Email Template** tab is displayed.



Note: Admins can create new user templates in the **Platform** module in AppViewX. For navigation and instructions to create a new email template, click here.

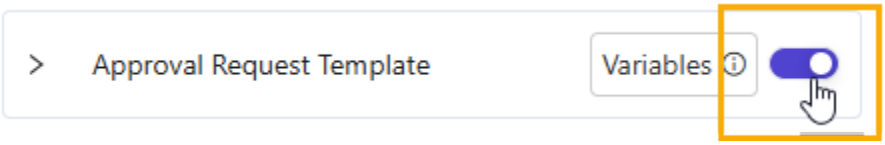
b. Select the rquired **Email Template** from the dropdown.

c. Policy Central includes templates for three types of approval -related emails:

- **Approval Request Template** (Sent to the approver when a request needs approval)
- **Approval Confirmation Template** (Sent to the requester when the request is approved)
- **Approval Rejection Template** (Sent to the requester when the request is rejected)

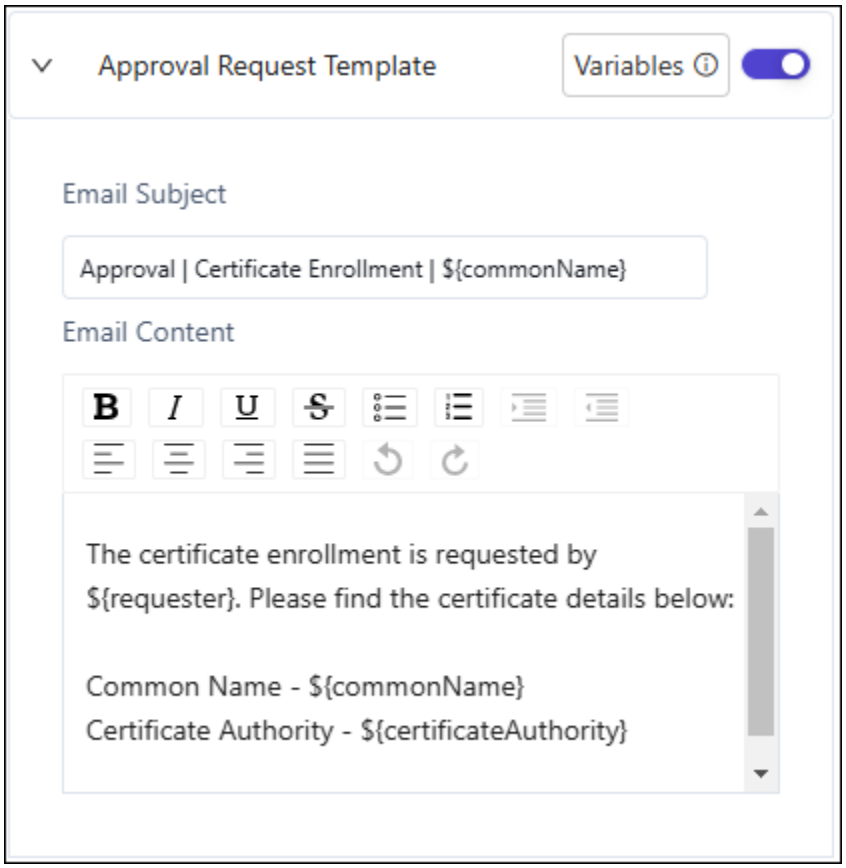
d. To customize the email templates in Policy Central:

e. To enable a template for editing, turn on the toggle button for the required template.



f. To view the email subject and body fields, click > .

The contents of the email are displayed.



g. To view the full list of variables that can be added to the email body, click **Variables**.
h. Using the variables and plain text values, customize the email subject and content, as required.
i. Click **Add**.

The contents of the email template are updated and saved.

Approval Execution & Notifications

Approvals are processed in two ways:

1. **Email-Based Approvals:** Approvers receive an email and can approve the request directly from their email.
2. **Appviewx Policy Central Execution Timeline View:** Approvers can log into AppViewX, navigate to **Policy Central → Policy Requests,** select the corresponding request, and approve it.

Approval Types and Execution Methods

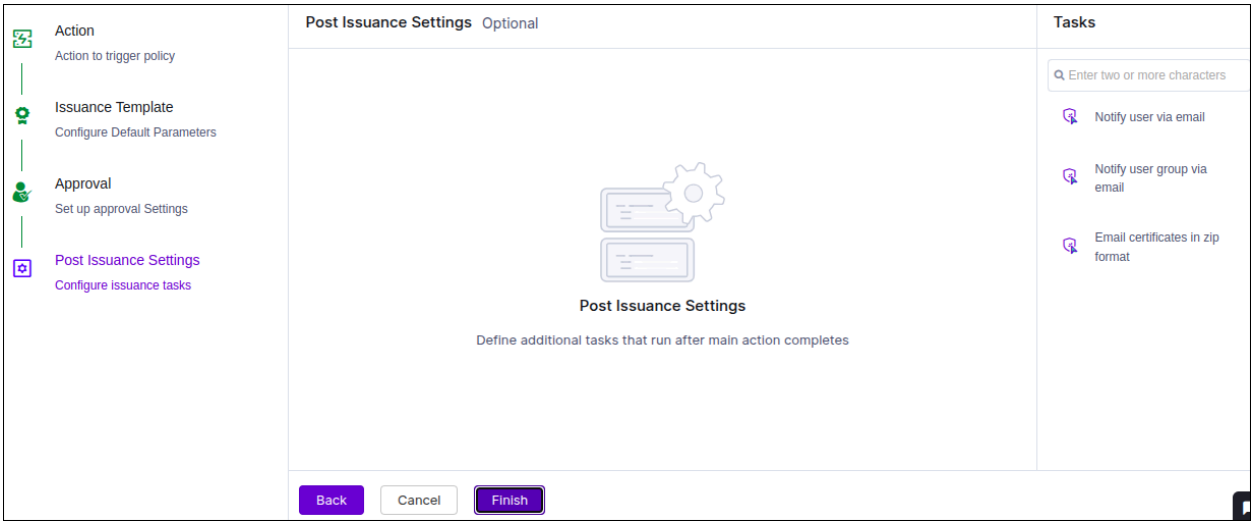
Approval Type	Approve via Email	Approve via Login
User	✓	✓
User Group	✓	✓
Email	✓	✗
LDAP Manager	✓	✓ (if part of AppViewX)

Notifications

For each approval action, a notification is sent to the requester. Currently, notifications are sent via **email**, with future support planned for **Slack**.

Post Issuance Settings (Optional)

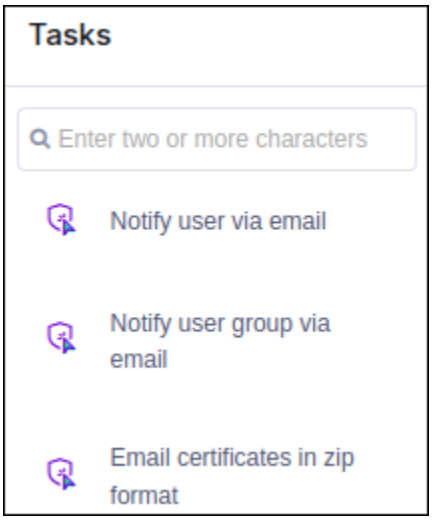
You can configure additional tasks to run after the main action is completed. Policy Central supports three post-action items, which are carried out once a policy is enforced.



Post action items are:

- Notifying users via email.
- Notifying user groups via email.
- Emailing certificates in the **.zip** format.

AppViewX Policy Central includes issuance templates for each of these actions.



Each action is customizable and is executed separately.

Configuring and Customizing the Tasks

Notifying Users via Email

1. On the **<policy name> :: Edit** page, under **Post Issuance Settings** > **Tasks**, select **Notify user via email**.

   The **Notify user via email** dialog box is displayed.

2. In the **Notify user via email** dialog box, from the **Notify user via email** dropdown list, select email addresses/names of one or more users to be notified of action completion.
3. Click **Confirm**.

   The Notify user via email task is displayed in the **Post Issuance Settings** page.

   Upon policy enforcement, all selected users will receive the corresponding email notification.

   Note: You can edit existing users or add new ones to the task by clicking the Edit icon, or delete the task by clicking the Delete icon.

Notifying User Groups via Email

1. On the **<policy name> :: Edit** page, under **Post Issuance Settings** > **Tasks**, select **Notify user group via email**.

   The **Notify user group via email** dialog box is displayed.

2. In the **Notify user group via email** dialog box, from the **Notify user group via email** dropdown list, select all user groups to be notified of action completion.
3. Click **Confirm**.

   The Notify user group via email task is displayed in the **Post Issuance Settings** page.

   Upon policy enforcement, all selected user groups will receive the corresponding email notification.

   Note: You can edit existing user group or add new user group to the task by clicking the Edit icon, or delete the task by clicking the Delete icon.

Emailed Certificates to the Requester

To receive certificates via email post action completion:

1. On the **<policy name> :: Edit** page, under **Post Issuance Settings** > **Tasks**, select **Email certificates in zip format**.

   The **Email certificates in zip format** dialog box is displayed.

2. In the **Email certificates in zip format** dialog box, from the **Certificate type** dropdown list, select the certificate type.

   Note: Only one certificate type can be selected at a time.

3. To also include the certificate chain when the certificates are emailed, select the **Include Root and Intermediate** checkbox.
4. Click **Confirm**.

   The Email certificates in zip format task is displayed in the **Post Issuance Settings** page.

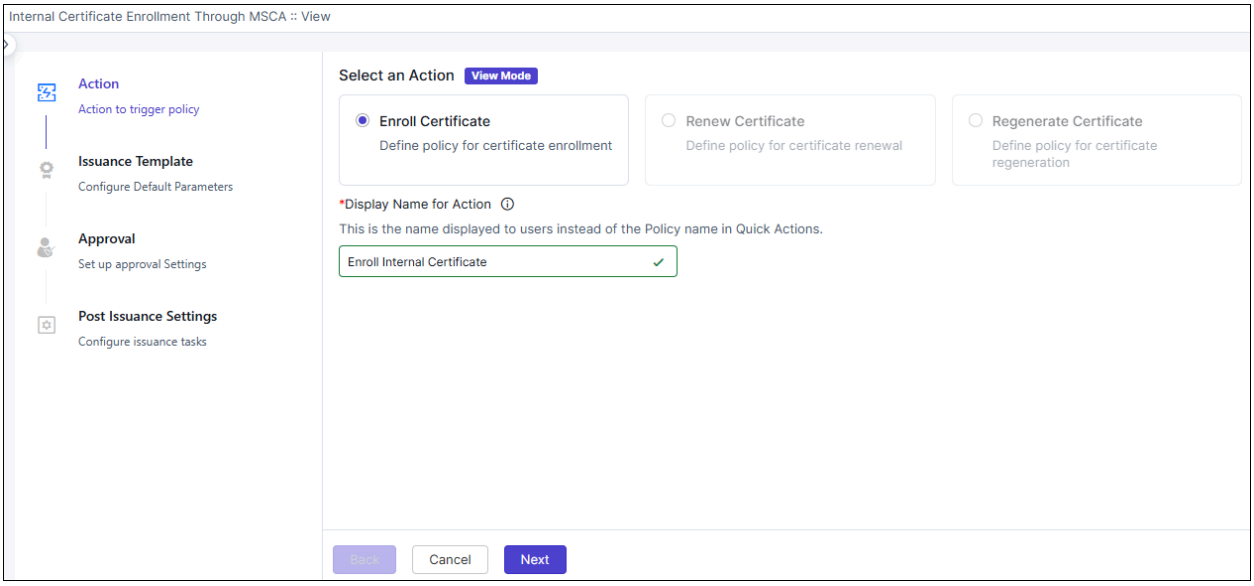
Upon policy execution, an email with certificates attached in the **.zip** format will be sent to the requester.

Note: You can change the zip format in the task by clicking the Edit icon, or delete the task by clicking the Delete icon.

Policy Actions

View Policy

Clicking on a policy name opens it in view mode, where detailed information about its configuration is displayed. This view includes the configured template details, outlining the policy's structure and parameters. Additionally, the view shows the supported post-actions, such as notifications.



Enable/Disable Policy

Once a policy is fully configured, it must be enabled using a toggle button to allow execution.

1. After a policy is fully configured, enable it by toggle button to allow execution under Status column.
2. Enabling the policy makes it available for use within the system.
3. When the policy is enabled, update and delete actions are restricted to prevent unauthorized modifications or accidental removals.
4. To make changes to the policy, it must first be disabled.
5. Disabling the policy allows modifications or deletion to be made.
6. This process ensures the integrity of the policy and maintains operational consistency.

User Access

Once a policy is created, it can be read (R) or modified (RW) by a user with the appropriate access. The User Access option allows granting access to the policy for various resources within an application.

By default, the resource associated with the policy creator is granted Read and Write (RW) permission, and this access cannot be modified later. Other resources can be granted Read (R) or Read and Write (RW) access, and these permissions can be modified at any time.

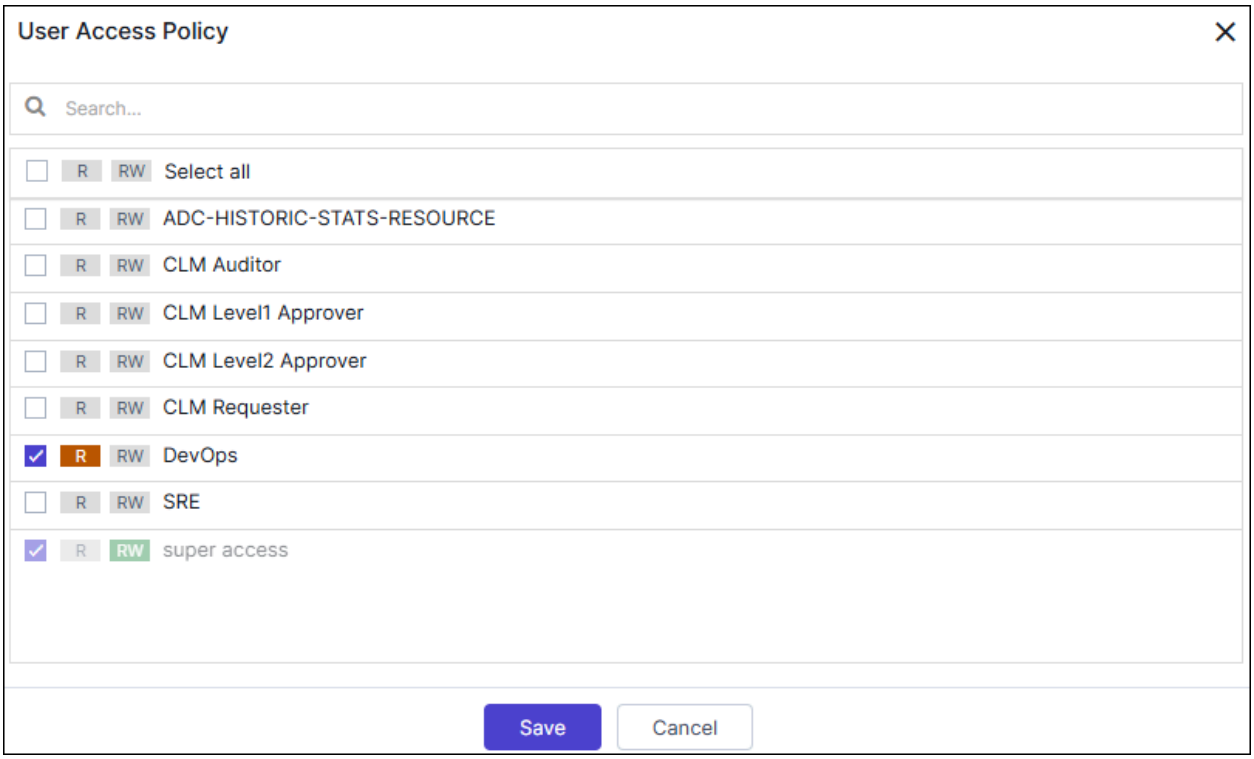
A user with Read (R) access to a policy can:

- View the policy
- Execute the policy
- Approve or reject a policy approval request.

A user with Read-Write (RW) access to a policy can:

- Edit the policy
- View the policy
- Execute the policy
- Approve or reject a policy approval request.

Note: Approvers must have Read (R) access to approve or reject requests.



To provide **User Access** to a policy:

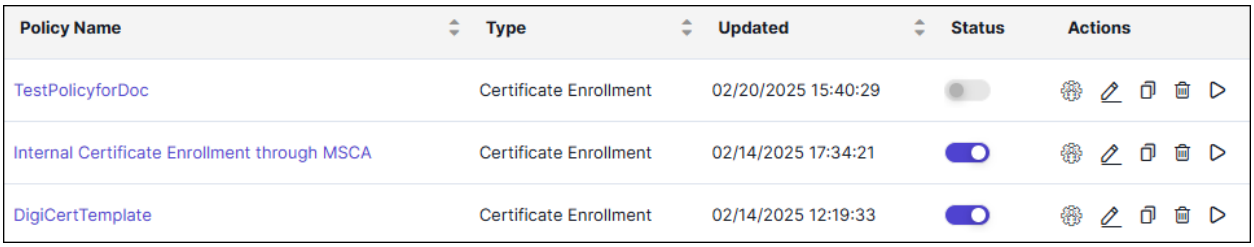
1. On the **Policy Inventory** page, below the actions column.
2. Click **(User Access)** icon.

   The **User Access Policy** page is displayed.
3. Select the checkbox for the required user access.
4. Click **Save**.

   The selected User Access is updated successfully.

Edit Policy

Once a policy is created, users with Read and Write (RW) access can modify its details using the Edit option. Clicking on Edit allows the user to change any part of the policy, just as they did during the creation process. The Edit option is only visible to users with RW access.



To Edit a policy:

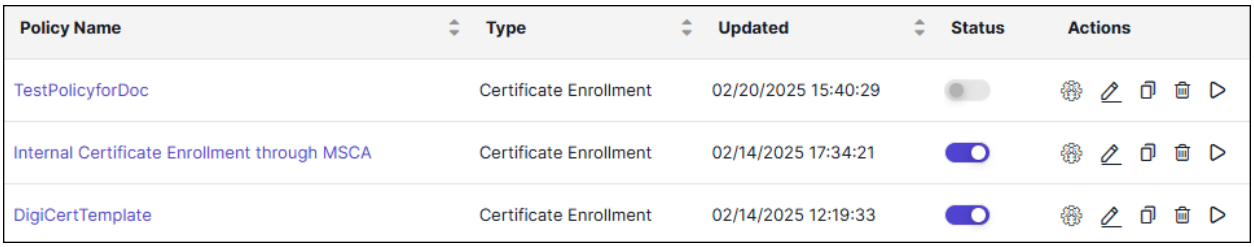
1. On the **Policy Inventory** page, below the actions column.
2. Click **(Edit Policy)** icon.

   The **[Policy Name] :: Edit** page is displayed.
3. Modify the required details in the **Action**, **Issuance Template**, **Approval** and **Post Issuance Settings** sections.
4. Click **Save**.

   The selected Policy is modified.

Clone Policy

A user can clone a policy, and all its properties and components will be duplicated in the cloned policy. The user can then make any necessary modifications to the cloned policy.



To clone a policy:

1. On the **Policy Inventory** page, below the actions column.
2. Click **(Clone Policy)** icon.

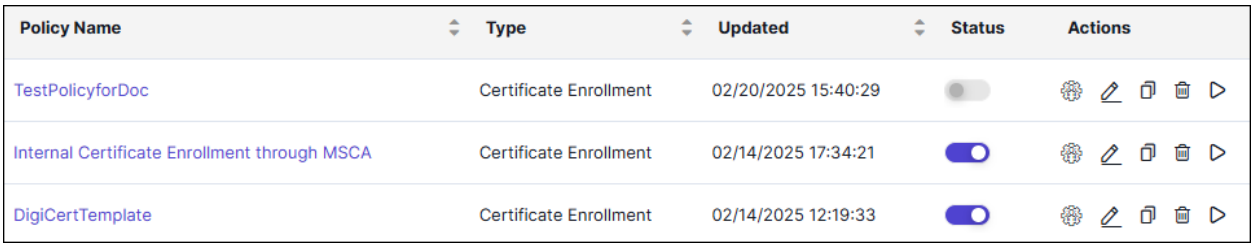
   The **Clone Policy** popup is displayed.
3. Enter the new **Policy Name**, **Description**, and **Select a Tag** for the policy.
4. Click **Clone Policy**.

   The selected policy is cloned.

Delete Policy

A user can delete a policy, but it must be in a disabled state before deletion. Once deleted, all information related to the policy will be removed.

However, if the policy has been created and executed by a user, its ACL will be retained to ensure smoother execution. Additionally, the execution history will be preserved for users to view.



To delete a policy:

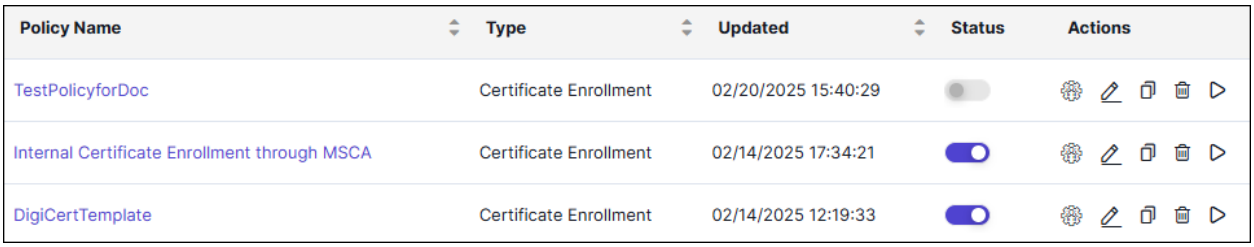
1. On the **Policy Inventory** page, below the actions column.
2. Click **(Delete Policy)** icon.

   The **Delete Policy** popup is displayed.
3. In the **Confirmation** dialog box, click **Confirm**.

   The selected policy is deleted successfully.

Execute Policy

After creating a policy, the Execute action enables the user to test the policy enforcement. A form based on the policy will be generated for the user to complete and submit. Execution details can be viewed on the Policy Requests page.



To execute a policy:

1. On the **Policy Inventory** page, below the actions column.
2. Click **(Execute Policy)** icon.

The **Policy Details** popup is displayed.

3. Update the **Certificate Parameters** details.
4. Click **Submit**.

The selected policy is executed successfully.

Creating a Cluster Policy Using Policy Central

Use **Policy Central** for a smarter, rule-based approach to policy creation. Predefined templates make it quick and easy to create and manage policies.

Prerequisites:

- Ensure CA integration is completed.
- Ensure you configured organization PKI standards as CA Policy.
- Ensure the Group is created.

To create a cluster policy:

1. Go to **Menu** > **KUBE+** > **GROUPS & POLICIES** > **Cluster Policy**
   On the **Cluster Policy** page, the existing policies (if any) are listed.
2. Click **+Create Policy** in the command bar.
   The **Cluster Policy** popup opens.
3. Under the **Policy Central** section, click **+Create Policy**.
4. In the **Welcome to Policy Central** popup, click **Get Started**.
5. In the **Create Policy** window:

   a. Select **Kube Cluster Policy** from the Policy Type dropdown.

   b. Fill in the policy details:

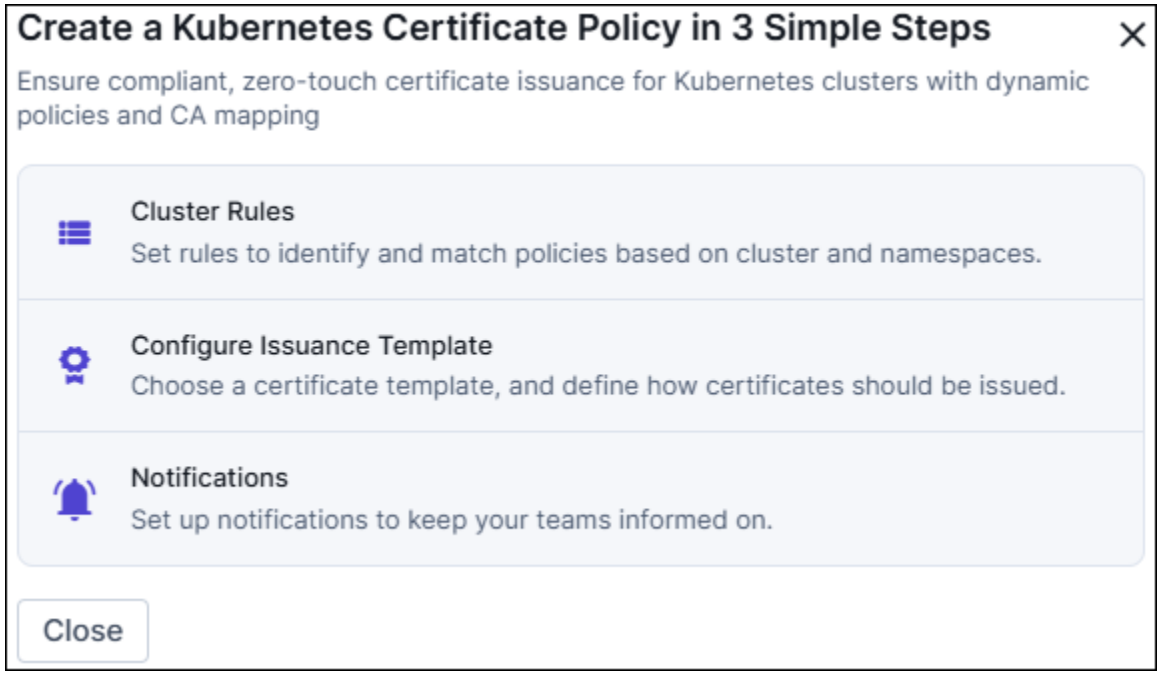
Policy Details - Field and Description Table

Field	Description
***Policy Name**	Enter a unique policy name to be associated with one or more clusters.

Field	Description
	Note: Enter a policy name that can include lowercase alphanumeric and the special characters -.
Description	Optionally, provide a brief description of the policy for clarity and reference.
***Select a Tag**	Choose a tag to categorize and manage the policy.
**: Mandatory fields*	

6. Click **Configure Policy**.

   The **Create a Kube Cluster Policy in 3 Simple Steps** popup displayed:



   - You may close it.
   - To avoid seeing it again, check **Don't Show Again**, then click **Close**.

7. Configuring the Policy as follows:

a. In the **Cluster Rules** page:
   - A default template is displayed. You can:
     - Use the existing template.
     - Modify and save it.
     - Save it as a new template.
   - Templates are listed under **Cluster Rule Templates** in the right panel.
   - Select a template to apply it to your rule.

b. The field in the **Cluster Rules** are:

Cluster Rules - Field and Description Table

Policy Application Scope	• **Cluster Wide** - Cluster wide global policy. • **Namespace Specific** - Policy to be applied for a specific namespace or a project within a cluster.
Policy Rules	Enable or disable the following rules as needed: • **Onboarding Rule** - Automatically map the policy by evaluating the configured rules when new clusters or namespaces are detected. If not enabled, the policy will not be mapped automatically but still can be mapped manually in KUBE+. • **Namespace Exclusion for Certificate Discovery** - Skip specified namespaces during the certificate discovery process. • **Off-boarding Rule** - Execute defined actions when clusters are removed from KUBE+.

8. Click **Next**.
9. In the **Issuance Template** page:
   - Select a certificate template from the right panel.
   - In the **Import Issuance Template** popup, click **Confirm**.
   - (Optional) Click **+ Add CA** to add more CAs, and fill in the required fields.
10. Click **Next**.
11. (Optional) Configure Notifications as follows:

a. On the **Notification (Optional)** page, click **+ Add Notification**.

b. In the **Configure Notification** panel, fill in the following:

Notification Settings Tab

Notification Settings - Field and Description Table

Field	Description
Recipient	Select recipients. The options are: • **User Group** - select this checkbox and add user groups from the dropdown list. • **User** - select this checkbox and add users from the dropdown list. • **Email** - enter the email address with comma separated.
Delivery Method	Select delivery methods. The options are: • ***Notify Via** - Bydefault Email option is selected. • **Notify Me** - Enable this toggle button to notify you when the policy is executed.

Message Template tab

Message Template - Field and Description Table

Field	Description
Email Template	Select a emal template from the dropdown list.
Email Subject	Enter the email subject. You can include variable to replace the value. To know about the variables, click Variables.
Email Content	Enter the email content for the bosy of the email. You can also use variables.

c. Click **Add**.

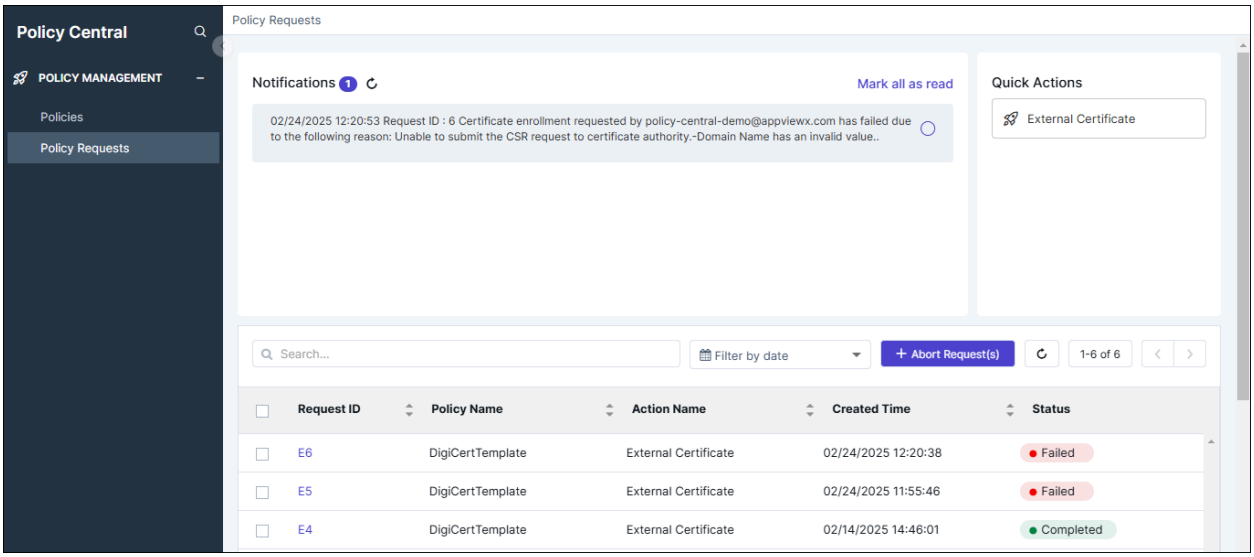
12. Click **Finish**.
13. In the **Submit Policy** confirmation popup, click **Confirm**.
    The cluster policy is added to the Cluster Policy inventory.

Related Information

- **Modifying Cluster Policy**

Chapter 5: Policy Requests

To access the policy request inventory, go to (**Menu**) > **Policy Central** > **POLICY MANAGEMENT** > **Policy Requests**.

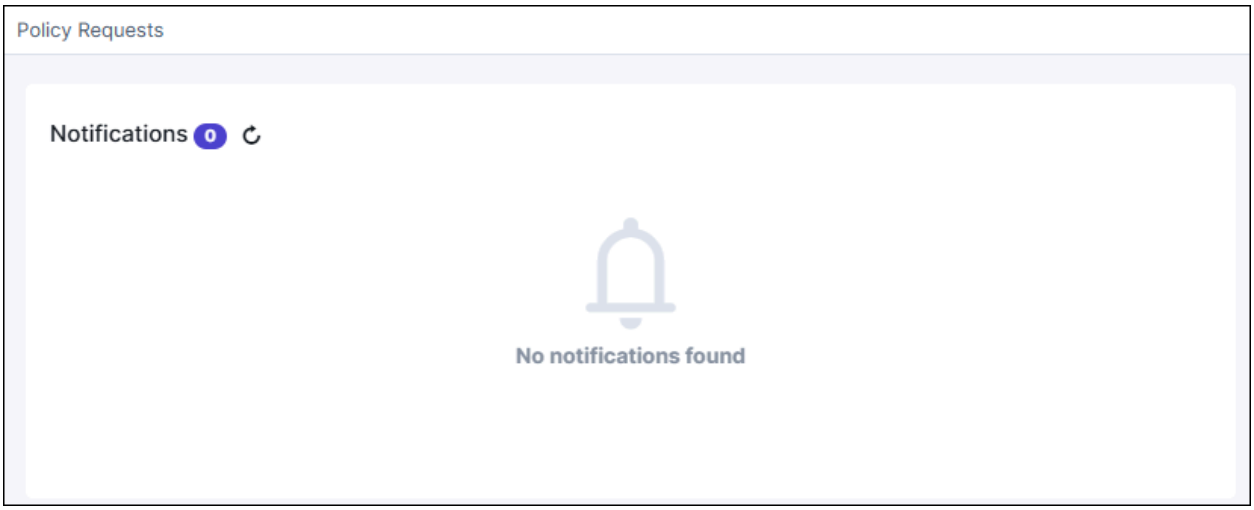


Notifications

The **Notifications** system provides real-time updates on policy requests, approvals, failures, and completions. The notification system ensures that **policy creators**, **requesters and approvers** receive timely updates and can take necessary actions.

To view these notifications, go to (**Menu**) > **Policy Central** > **POLICY MANAGEMENT** > **Policy Requests**.

The **Policy Requests** page, with the **Notifications** section is displayed.



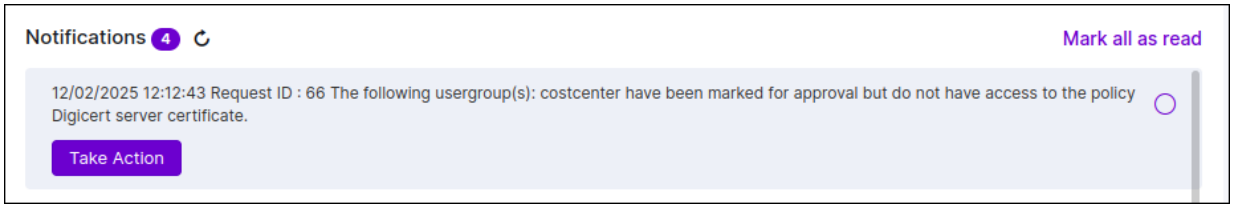
Understanding Notifications for User Roles

Policy Creator

The policy creator will receive notifications for the following events:

- **Approval Access Issue**

  If the approver does not have access to the policy requested by the user, the policy creator is notified.



  To grant the requisite permissions for the approver, click **Take Action** and update the policy access using the dialog box displayed.

Requester

The requester will receive notifications for the following events:

- **Approval/Rejection Notification**

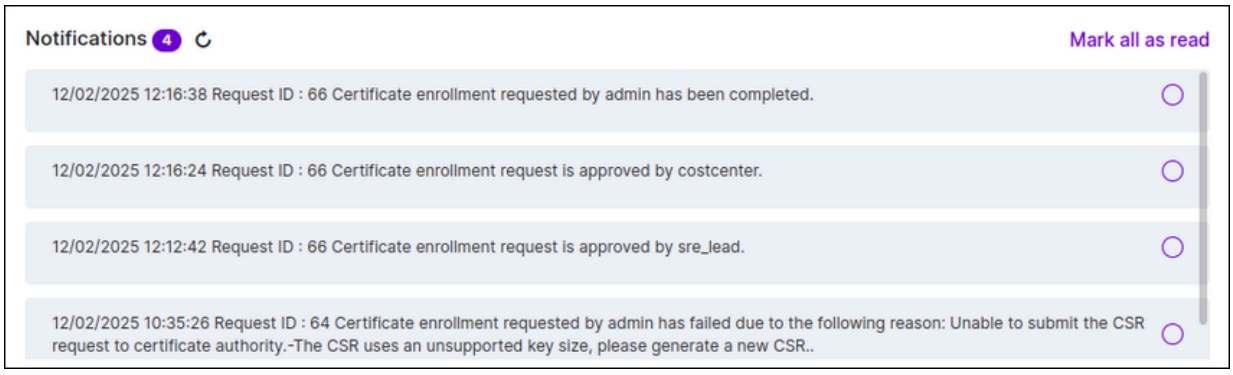
  Sent when the approver accepts/rejects the request.

- **Failure Notifcation**

  Sent to the requester if there has been a failure during policy execution.

- **Successful notification**

  Sent to the requester when the request has been executed successfully.



Approver

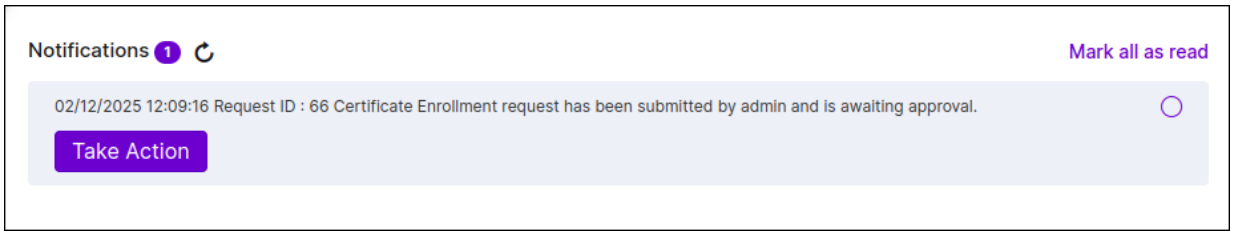
The approver will receive notifications for the following events:

- **Pending Approval Notification**

  The approver will receive a notifcation if a request is pending for approval.

  To review the approval request, click **Take Action** for the corresponding notifcation.

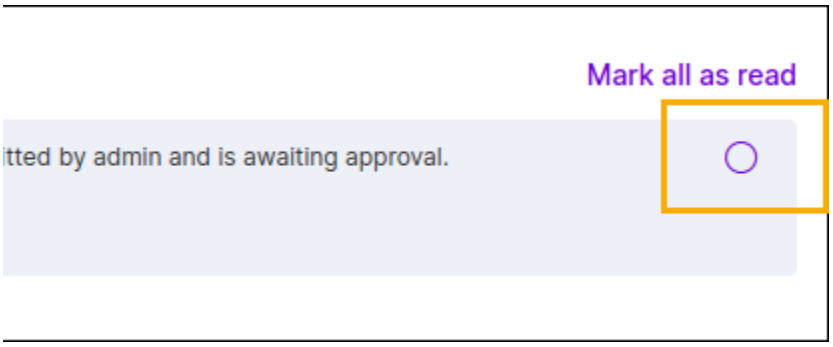
  You will be redirected to the request ID's timeline, where you can approve/reject the request.



Managing Notifications

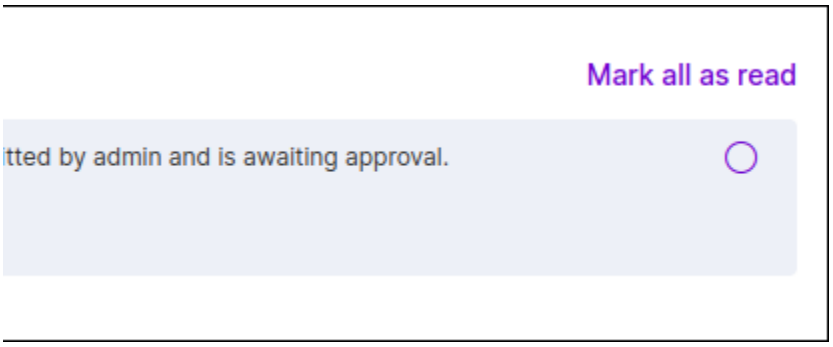
Marking individual notifications as read

To mark an individual notification as click ○ corresponding to the notification.



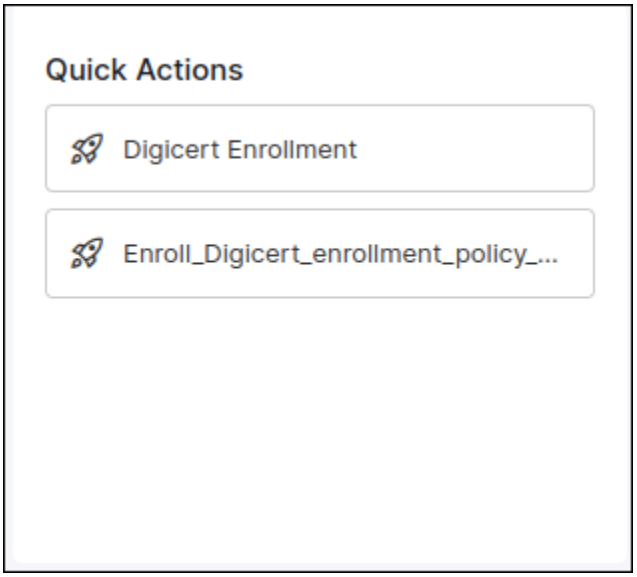
Marking all notifications as read

To mark all notifications as read, click **Mark all as read**.



Quick Links

The **Quick Actions** panel provides a convenient way to initiate policy executions. It displays a list of **Action Names** associated with policies, allowing users to quickly trigger executions.



Note: Only Active policies are displayed in Quick Actions.

Policy Execution Inventory

Understanding the Policy Execution Inventory

The **Policy Execution Inventory** is a list of all policy executions that includes key policy details as well as the search and abort functionalities, as explained below:

- **Request ID**: A unique identifier assigned to each policy execution for tracking purposes. Click the request ID to view the request timeline. To understand the request timeline details, click here.
- **Policy Name**: Name of the policy associated with the execution.
- **Action Name**: Name of the action associated with the policy, which is used to initiate the execution.
- **Created Time**: Timestamp of policy execution initiation.
- **Status**: Current status of the policy execution.

  The policy execution **Status** is indicated using the following values:

Status	Description
In Progress	Policy execution is in progress.
Waiting	Policy execution is pending approval or is waiting for certificate issuance.
Rejected	Policy execution request has been rejected by the approver.
Failed	Policy execution has encountered a system error or a failure scenario.
Aborted	Policy execution request has been aborted.
Completed	Policy execution has been successfully completed.

Searching for Execution Requests in the Inventory

To search for execution requests, you can:

- Use the **Search** field to search for execution requests by policy name, action name, and request ID.
- Use the **Filter by date** field to filter requests for a required timeline.

Aborting Policy Execution Requests

To abort policy execution request(s):

1. Select the checkbox corresponding to the execution request(s) you want to abort.
2. From the execution inventory, click **Abort Request(s)**.

Understanding the Request Timeline

When the **Request ID** is clicked, a timeline view of the execution request is displayed, showing the sequence of execution stages. The execution stages define the step-by-step process of handling a request. Each stage represents a distinct step, ensuring a clear progression from submission to final delivery.

Execution Stages

- **Certificate Enrollment Request**

  This stage displays all certificate parameters submitted by the user. It provides a summary of the request, including details such as certificate type, validity period, and associated metadata. This serves as the initial checkpoint before moving to the approval process.

- **Approval Levels**

  Each approval level is treated as a separate stage, displaying the approver responsible for reviewing and approving the request. Approver comments, if provided before approving or rejecting the request, are also displayed here.

  If multiple approval levels are configured (for example, Level 1 and Level 2), only the first level will be visible initially. Once the first level approval is obtained, the request will move to the next level, thus progressing until all required approvals are obtained.

- **CSR Creation**

  Once all approval levels are completed, the request proceeds to the Certificate Signing Request (CSR) creation stage. This stage displays details such as the Common Name (CN) for which the certificate is being requested.

- **Certificate Issuance**

  After CSR creation, the process moves to the certificate issuance stage. In this step, the certificate is generated and issued based on the provided details. Once issued, the certificate is ready for further actions.

Post Action Stages

Each post-action is treated as a separate stage and occurs only if it is configured. These stages define additional actions taken after certificate issuance. By default, the system automatically notifies the requester via email upon certificate issuance, but this notification is not considered part of the execution stages.

The three post-action stages supported in Policy Central are:

- **Email with certificate**

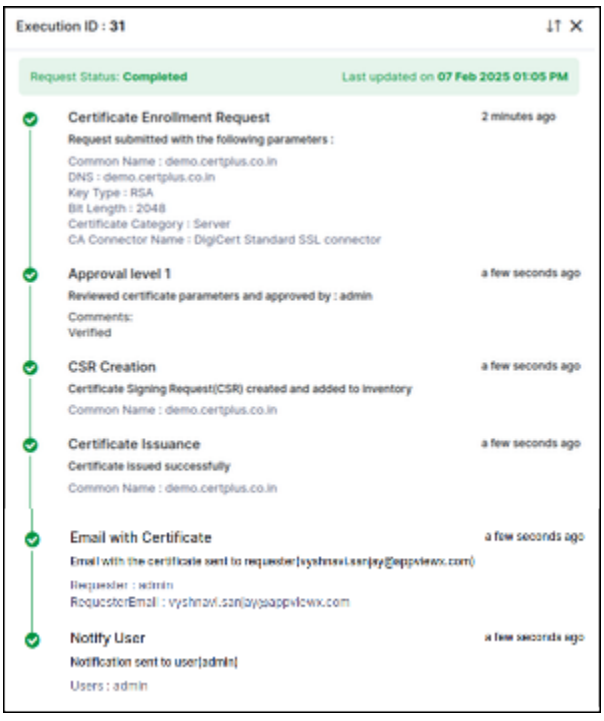
  This stage is triggered if the **Email certificates in zip format** post-action is configured. The system sends an email containing the issued certificate to the requester.

- **Notify users**

  If the **Notify users via email** post-action is configured, this stage sends an email notification to the selected user(s), informing that the certificate has been successfully issued.

- **Notify user groups**

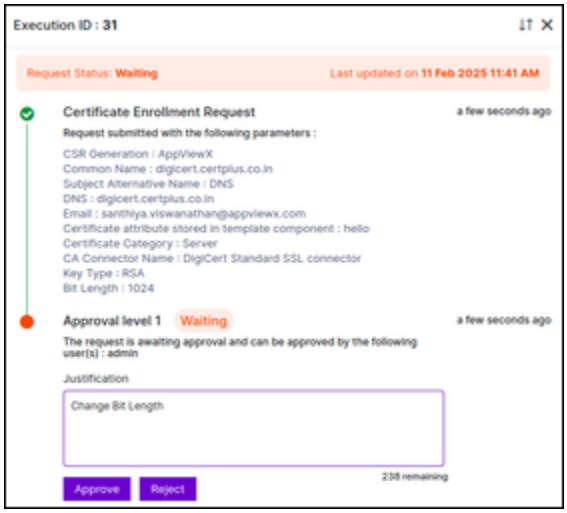
  If the **Notify user groups via email** post-action is configured, this stage sends an email notification to the selected user group(s), ensuring that relevant users are informed about the certificate issuance.



Actions

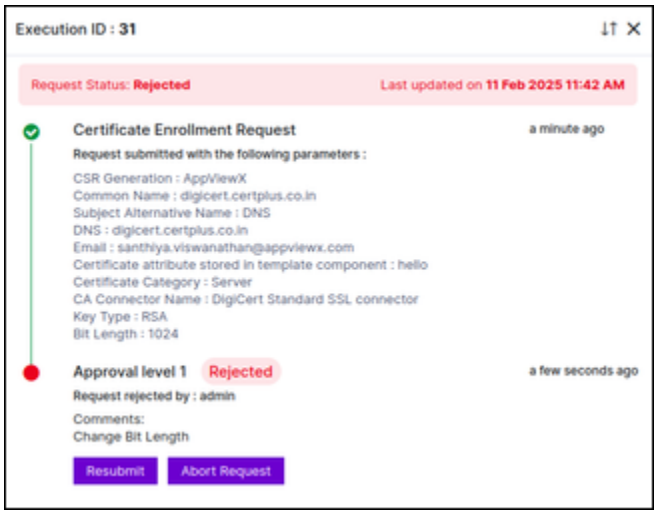
- **Approve and reject**

  Approvers with policy access can either approve or reject a request. If the **Allow Comments** option is enabled in the policy, approvers can provide comments explaining their decision. If the request contains incorrect details or does not meet the required criteria, the approver can reject it. However, if all parameters are valid, the request can be approved for further processing.



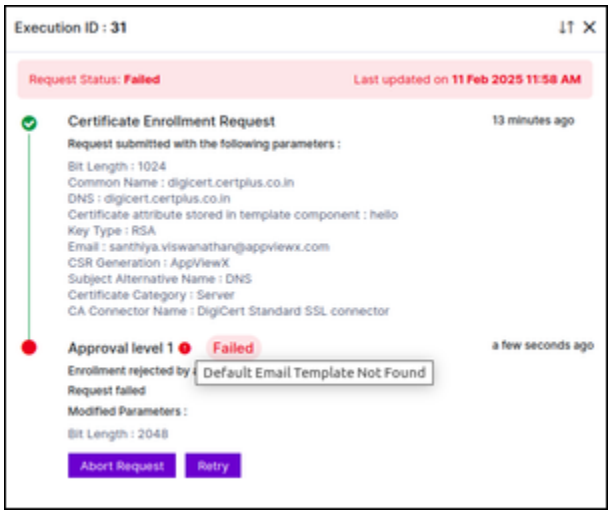
- **Resubmit**

  If a request is rejected, the requester can resubmit it after making necessary modifications, provided that **Allow Resubmission** is enabled in the policy. This ensures that rejected requests can be corrected and reconsidered without requiring a completely new submission.



- **Retry**

If a policy request fails due to system errors or other issues, the Retry action allows the request to be executed again. This ensures that temporary failures do not require a full resubmission and can be resolved efficiently. When a **stage fails**, an exclamation mark (!) indicator appears beside the failed stage. The **error message becomes visible only when hovering over the exclamation mark**.



- **Abort**

If a policy request is no longer required, it can be aborted to prevent further processing. However, once the request reaches the implementation stage (e.g., certificate issuance), the abort action is no longer allowed. This restriction ensures that partially executed processes are not left in an inconsistent state.

Transitions in Execution Stages

Execution progresses through the following stages:

1. **In Progress**

   Represents an active process that is being executed.

   Can transition to:
   - **Waiting** (if the request is awaiting approval or further execution steps)
   - **Failed** (if an error occurs)
   - **Completed** (if successfully processed)
2. **Waiting**

   Represents a paused process, either waiting for approval or for certificate issuance.

   Can transition to:

- **In Progress** (if the request has been approved or the certificate has been issued)
- **Rejected** (if approval is denied)
- **Aborted** (only if awaiting approval, not during certificate issuance)

3. **Rejected**

   Represents a rejected request.

   Can transition to:

   - **In Progress** (if resubmitted)
   - **Aborted**

4. **Failed**

   Represents a process that encountered an error.

   Can transition to:

   - **In Progress** (if retried)
   - **Aborted**

   This can also be a final state if retry is not possible.

5. **Aborted**

   Represents a process that is manually stopped.

   This is a terminal state.

6. **Completed**

   Represents a process that has successfully completed execution.

   This is a terminal state.

Chapter 6: FAQs

What is the difference between the CA Policy and the Certificate Policy?

The **Certificate Policy** feature in Policy Central allows for the configuration of certificate parameters, designation of approvers, and specification of actions to be taken after certificate issuance.

Should I configure a CA Policy even though I’m using a Certificate Policy in Policy Central?

A CA policy must be configured to control aspects such as generating compliance reports and controlling private key downloads, as well as to identify non-compliant certificates. While the certificate policy in Policy Central can set guidelines and enforce them during certificate enrollment, it does not cover all the features supported by CA policy.